# CCTV: DEVELOPING PRIVACY BEST PRACTICES

**DECEMBER 17 and 18, 2007** – *Day One*

Hilton Arlington

950 North Stafford Street, Arlington, Virginia

Homeland Security

## The Privacy Office

U.S. Department of Homeland Security
Washington, DC 20528
t: 703-235-0780; f: 703-235-0442
privacy@dhs.gov; www.dhs.gov/privacy

# Technology Perspectives

## CCTV Technology

**Larry S. Davis**
Chair and Professor
Dept. of Computer Science, University of Maryland

Homeland Security

# The present and future of wide area visual surveillance systems

Larry Davis
Computer Science Department
Institute for Advanced Computer Studies
University of Maryland
College Park, Maryland 20742

# What do current visual surveillance systems do?

- Intrusion detection for perimeter and facility security
- Detection of anomalous behavior (vehicles driving erratically, ships out of their lanes).
- Person authentification – face/iris detection and face/iris recognition
- Limited change detection (left package detection)

# What are future applications?

- Tracking people and vehicles through city wide networks of cameras
  - Currently done manually
- Video forensics
- Detection of suspicious human behavior
  - Immigration screening
  - Crime detection
- Detection of activity networks – collections of people, places and vehicles involved in dangerous activity
  - IED manufacturing and emplacement

# Privacy protection and visual surveillance

- How can we protect privacy of people as camera networks proliferate?
- Blur faces/license plates or other “biometrics”
  - Destructive – can’t recover the face after the image has been blurred

    Well, that is not completely true – progress on video super-resolution might allow someone to recover a face from a sequence of blurred images of the face

# Privacy protection and visual surveillance

- Solution is provided by public key cryptography
  - Same technology as is used for secure communication over the internet
  - The face region is encrypted using a secret key – and it looks like a scrambled face so is unrecognizable by a person
    - And cannot be recovered by any combination of encrypted faces from a long video
  - Subsequently, the face can be recovered if the secret key is made available
    - After certain legal processes are followed.

# Privacy protection and visual surveillance

- There are still remaining problems
  - Face detectors make mistakes, and miss faces
    - They would not be encrypted, so would be visible to operators.
  - There are other (weaker) biometrics which are not easily hidden and could be used for identification
    - Body size and shape
    - Gait
    - Hair